



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/936,834

03/12/2002

Thomas Breitbach

RIEB.P-44

1508

28752 7590 09/06/2007  
LACKENBACH SIEGEL, LLP  
LACKENBACH SIEGEL BUILDING  
1 CHASE ROAD  
SCARSDALE, NY 10583

EXAMINER

LU, ZHIYU

ART UNIT

PAPER NUMBER

2618

MAIL DATE

DELIVERY MODE

09/06/2007

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	Application No. 09/936,834	Applicant(s) BREITBACH ET AL.	
	Examiner Zhiyu Lu	Art Unit 2618	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 26 June 2006.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1 and 20-37 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1 and 20-37 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)          | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |

**DETAILED ACTION**

***Response to Amendment***

1. Claims 1 are 20-37 pending, which is filed 06/26/2006.

***Response to Arguments***

2. Applicant's arguments with respect to claims 1 and 20-37 have been considered but are moot in view of the new ground(s) of rejection.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1, 20-28, 30-31, 34 and 36-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hultgren (US Patent#6868391) in view of "HBCI HOMEBANKING COMPUTER INTERFACE – Interface Specification – Version 2.1" (hereafter, HBCI) and "At the Coal-face Between Financial Industries and Politics" (hereafter, Interview w/ CG).  
Regarding claim 1, Hultgren teaches a method for using standardized bank services via mobile radiotelephone within a GSM mobile system with Telepay banking standard, comprising the

steps of transmitting between a bank server and a mobile station builds on a transmission method:

inserting an Telepay gateway (30 of Fig. 1A) into the Telepay transmission path between the bank server (80 of Fig. 1A) and the mobile station (60 of Fig. 1A), which carries out a transformation between Telepay transmission method used at the bank end and a transmission method used at the radiotelephone end (column 3 line 39 to column 4 line 47); and

splitting of the customer-end system into two components, a SIM card of the mobile station and the Telepay gateway (Fig. 1A, column 12 line 59 to column 13 line 21).

Hultgren differs from the present invention is that Hultgren used the Telepay gateway between the bank and the GSM mobile network instead of a HBCI gateway.

HBCI is a well known standardized bank-independent protocol for online banking, developed and in use by German banks, which provides support for multibanking, platform-independent, and DES- and RSA-encryption and –signatures with chip card (HBCI, Chapters I & VIII.8, especially VIII.8.4)

Further, Interview w/ CG teaches that with GSM network anyone could design using one of OFX, Integrion Gold, and HBCI as design preference for adapting European Internet banking standard in international network banking implementation (pages 1-11, especially 21<sup>st</sup>-22<sup>nd</sup> of Q&G). Thus, one of ordinary skill in the art can implement HBCI gateway between the GSM network and the banks (as shown in Interview w/ CG). The implemented network can be used in GSM mobile network with the European banks. The implemented network will also function necessary step such as splitting the customer-end system into GSM and HBCI. In US, Telepay

banking standard can be implemented with a GSM mobile network, which is shown in the Hultgren reference.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to make use of HBCI gateway instead of Telepay gateway of Hultgren as design preference as evidenced by Interview w/ CG, in order to perform Internet banking with European banks over GSM network.

Regarding claim 37, Hultgren teaches a method for using standardized bank services via mobile radiotelephone, comprising the steps of

transmitting data between a bank server (80 of Fig. 1A) and a mobile station (60 of Fig. 1A) builds on a Telepay transmission method (Fig. 1A);

inserting an Telepay gateway (30 of Fig. 1A) into the transmission path between the bank server and the mobile station, which carries out a transformation between the Telepay transmission method used at the bank end and a transmission method used at the radiotelephone end (column 3 line 39 to column 4 line 47);

splitting the customer-end Telepay system into two components, a SIM card of the mobile station and the Telepay gateway (Fig. 1A, column 12 line 59 to column 13 line 21);

forming two transmission routes, the first between a SIM card and the Telepay gateway and the second between the Telepay gateway and a bank server (Fig. 1A, column 12 line 59 to column 13 line 21); and

unpacking an Telepay protocol by the Telepay gateway and converting its protocol sequence such that compatibility with a GSM SIM card and a GSM network is obtained so that an exchange of the converted protocol with the GSM SIM card is possible (inherent).

Hultgren differs from the present invention is that Hultgren used the Telepay gateway between the bank and GSM mobile network instead of a HBCI gateway.

HBCI is a well known standardized bank-independent protocol for online banking, developed and in use by German banks, which provides support for multibanking, platform-independent, and DES- and RSA-encryption and –signatures with chip card (HBCI, Chapters I & VIII.8, especially VIII.8.4)

Further, Interview w/ CG teaches that with GSM network anyone could design using one of OFX, Integriion Gold, and HBCI as design preference for adapting European Internet banking standard in international network banking implementation (pages 1-11, especially 21<sup>st</sup>-22<sup>nd</sup> of Q&G). Thus, one of ordinary skill in the art can implement HBCI gateway between the GSM network and the banks (as shown in Interview w/ CG). The implemented network can be used in GSM mobile network with the European banks. The implemented network will also function necessary step such as splitting the customer-end system into GSM and HBCI. In US, Telepay banking standard can be implemented with a GSM mobile network, which is shown in the Hultgren reference.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to make use of HBCI gateway instead of Telepay gateway of Hultgren as design preference as evidenced by Interview w/ CG, in order to perform Internet banking with European banks over GSM network.

Regarding claim 20, Hultgren, HBCI, and Interview w/ CG teach the limitation of claim 1.

Hultgren teaches wherein two transmission routes are formed, first between a SIM card and the HBCI gateway and second between the HBCI gateway and a bank server (Fig. 1A of Hultgren).

Regarding claim 21, Hultgren, HBCI, and Interview w/ CG teach the limitation of claim 1.

Hultgren, HBCI, and Interview w/ CG teach the method of utilizing HBCI banking over GSM network, which would have been obvious to one of ordinary skill in the art at the time the invention was made to recognize that an HBCI protocol is unpacked by the HBCI gateway and its protocol sequence is converted such that compatibility with a GSM SIM card and a GSM network is obtained in order for an exchange of the converted protocol with the GSM SIM card is to be possible.

Regarding claim 22, Hultgren, HBCI, and Interview w/ CG teach the limitation of claim 1.

Hultgren teaches a carrier service for the information exchange to be short message service (column 13 lines 22-32).

Regarding claim 23, Hultgren, HBCI, and Interview w/ CG teach the limitation of claim 20.

Hultgren teaches on both routes a cryptographic security is realized (column 6 lines 38-43, column 12 lines 59-65).

Regarding claim 24, Hultgren, HBCI, and Interview w/ CG teach the limitation of claim 1.

Hultgren, HBCI, and Interview w/ CG teach wherein between the bank server and the HBCI gateway a security protocol defined by is applied HBCI (III.1.3 of HBCI) and between the HBCI gateway and a SIM card a second security protocol is employed (column 12 line 59 to column 13 line 63 of Hultgren).

Regarding claim 25, Hultgren, HBCI, and Interview w/ CG teach the limitation of claim 24.

Hultgren, HBCI, and Interview w/ CG teach wherein the second security protocol corresponds to a protocol reduced in terms of data quality where the transmission only deals with a single customer, but equivalent to HBCI in terms of security technology (III.1.3), where encryption algorithm to be used is by customer's preference and supported by the bank to fit for security procedure and compression procedure of HBCI.

Regarding claim 26, Hultgren, HBCI, and Interview w/ CG teach the limitation of claim 25.

Hultgren, HBCI, and Interview w/ CG teach a cryptographic key ( $K_{sms}$ ) (signature key of HBCI) specific to each subscriber is securely generated and stored in a SIM card (Chip card of Fig. 1 of HBCI; 62 of Fig. 1A of Hultgren) for use in the second security protocol after regular SIM card personalization (I, VI.3.1.1 Key types of HBCI).

Regarding claim 27, Hultgren, HBCI, and Interview w/ CG teach the limitation of claim 1.

Hultgren, HBCI, and Interview w/ CG teach wherein the generation of the key ( $K_{sms}$ ) specific to the subscriber is generated in the SIM card by entering an initialization PIN on the mobile

telephone (VI.3 of HBCI), where using two or more keys to generate a specific key is also well known in the art of cryptography.

Regarding claim 28, Hultgren, HBCI, and Interview w/ CG teach the limitation of claim 1. HBCI teaches wherein a subscriber is informed per PIN letter by the bank of a PIN for generating the key (Ksms) (VI.3.1.3.2 Initial key distribution, in writing from the bank).

Regarding claim 30, Hultgren, HBCI, and Interview w/ CG teach the limitation of claim 1. HBCI teaches wherein before subscription to a service a subscriber receives the data of his bank including an initialization PIN (User ID of III.1.1, VI.3.1.3.2 Initial key distribution).

Regarding claim 31, Hultgren, HBCI, and Interview w/ CG teach the limitation of claim 30. HBCI teaches a cryptographic method of generating the key through triple DES using country code (local PIN), bank code (routing number), user ID (account number), key type, key number, and version number (VI.3.1.1, II.5.3.2), which means during the initialization of an application, i.e. during subscription, with the aid of the KIV from initialization PIN, the key Ksms is generated through triple DES using the local PIN, the bank routing number and an account number.

Regarding claim 34, Hultgren, HBCI, and Interview w/ CG teach the limitation of claim 1.

Hultgren, HBCI, and Interview w/ CG teach wherein the authentication of the two involved sites, mobile radiotelephone subscriber and HBCI gateway, takes place by knowledge of the initialization PIN exchanged in writing (VI.3.1.3.2 of HBCI).

Regarding claim 36, Hultgren, HBCI, and Interview w/ CG teach the limitation of claim 1. Hultgren teaches wherein an additional authentication of a subscriber takes place via an identification of his/her mobile connection to carry out an evaluation of a calling line identification (CLI) (column 13 lines 33-49).

4. Claims 29 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hultgren (US Patent#6868391) in view of “HBCI HOMEBANKING COMPUTER INTERFACE – Interface Specification – Version 2.1” (hereafter, HBCI), “At the Coal-face Between Financial Industries and Politics” (hereafter, Interview w/ CG), and Atalla (US Patent#4288659).

Regarding claim 29, Hultgren, HBCI, and Interview w/ CG teach the limitation of claim 1. But, Hultgren, HBCI, and Interview w/ CG do not expressly disclose during a card personalization by the mobile telephone network operator together with the bank application, an initialization key KIV, derived from a master key and a SIM card-individual number, for generating a Ksms specific to the subscriber is applied onto a plurality of SIM cards. Atalla teaches generating an initialization key based on a secret code (master key) known by both authorized individual and the bank and an identification of the terminal for generating the

Art Unit: 2618

session key specific to the terminal user (column 1 line 45 to column 2 line 27), where applying the key generating method is obvious to one of ordinary skill in the art to apply on other cards as well.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate generating initialization key from a master key and a hardware individual number taught by Atalla into the method of Hultgren, HBCI, and Interview w/ CG, in order to provide both user and hardware authentication in initialization.

Regarding claim 33, Hultgren, HBCI, and Interview w/ CG teach the limitation of claim 1.

But, Hultgren, HBCI, and Interview w/ CG do not expressly disclose the generation of an initialization PIN takes place at the HBCI gateway and this is transferred to the bank server.

However, it is known that the gateway is a mid-node for authentication and conversion for user data before communicating with the bank. So, the gateway would be the one who masters security with the user and the bank, which would have been obvious to one of ordinary skill in the art to recognize that having the gateway to generate initialization PIN is secure and convenient. Then initialized PIN can be transferred to the bank so that the bank can inform user the initialization key since the bank is the one who authorize the service.

Atalla teaches the generation of the initialization PIN takes place at the terminal (mid-node between user and bank) and data terminal must be initialized in the first operating cycle (column 1 line 45 to column 2 line 27, column 2 lines 64-67).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate generating initialization key in mid-node taught by Atalla into the

method of Hultgren, HBCI, and Interview w/ CG, in order to provide secured user initialization and authentication in the HBCI gateway.

5. Claim 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hultgren (US Patent#6868391) in view of “HBCI HOMEBANKING COMPUTER INTERFACE – Interface Specification – Version 2.1” (hereafter, HBCI), “At the Coal-face Between Financial Industries and Politics” (hereafter, Interview w/ CG), and Fujioka (JP10-242957).

Regarding claim 32, Hultgren, HBCI, Interview w/ CG, and HBCI Specification v2.1 teach the limitation of claim 27.

But, Hultgren, HBCI, Interview w/ CG, and HBCI Specification v2.1 do not expressly disclose wherein in the generation of the Ksms in the HBCI gateway an initialization PIN is transferred to a gateway operator.

Fujioka teaches transferring an initial key to server for generating another key (abstract).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate transferring initialization PIN to server for generating a key taught by Fujioka into the modified method of Hultgren, HBCI, Interview w/ CG, and HBCI Specification v2.1, in order to authenticate key generation for corresponding client.

6. Claim 35 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hultgren (US Patent#6868391) in view of “HBCI HOMEBANKING COMPUTER INTERFACE – Interface

Art Unit: 2618

Specification – Version 2.1” (hereafter, HBCI), “At the Coal-face Between Financial Industries and Politics” (hereafter, Interview w/ CG), and Elgamal et al. (US Patent#5657390).

Regarding claim 35, Hultgren, HBCI, and Interview w/ CG teach the limitation of claim 1.

But, Hultgren, HBCI, and Interview w/ CG do not expressly disclose between mobile radiotelephone network operator and HBCI gateway operator a master key is exchanged.

Elgamal et al. teach between mobile radiotelephone network operator and HBCI gateway operator a master key is exchanged (column 7 lines 41-56).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate exchanging master key taught by Elgamal et al. into the method of Hultgren, HBCI, and Interview w/ CG, in order for both client and server to produce session keys for encrypt/decrypt data during communication.

### *Conclusion*

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zhiyu Lu whose telephone number is (571) 272-2837. The examiner can normally be reached on Weekdays: 9AM-5PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nay Maung can be reached on (571) 272-7882. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2618

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Zhiyu Lu  
August 23, 2007

  
**NAY MAUNG**  
**SUPERVISORY PATENT EXAMINER**